IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (currently amended)A symmetric-key encryption method performed by a computer comprising the steps of:

dividing plaintext composed of a message and redundancy data added to the message ~~and a message~~ to generate a plurality of plaintext blocks each having a predetermined length, wherein the redundancy data is added to detect whether a ciphertext obtained from said plaintext has been altered;

~~generating a random number sequence based on a secret key;~~

generating a first random number block and a second random number block both corresponding to each ~~one~~ of said plurality of plaintext blocks based on a secret key that is an input value~~from said random number sequence~~;

performing encrypting operations for producing ciphertext blocks each corresponding to each of said plurality of plaintext blocks; and

concatenating the series of said ciphertext blocks one after another sequentially to output said series as said ciphertext,

wherein one of said encryption operations for producing the ciphertext block i corresponding to the plaintext i (2 $\leqq$i$\leqq$ a number of plaintext blocks) comprises:

a first operation step for performing an arithmetic computation on said plaintext block i and said first random number block corresponding to said plaintext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said plaintext block i and said second random number block corresponding to said plaintext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said plaintext block i and a result of said first operation step performed on said plaintext block i-1, to produce said ciphertext block i, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of plaintext blocks or the result of said second operation step.~~outputting a feedback value obtained as a result of operation on said one of said plurality of plaintext blocks and said random number block, said feedback value being fed back for use in the operation on another one of said plurality of plaintext blocks; and~~

~~performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of said plurality of plaintext blocks to produce a ciphertext block.~~

2. (currently amended)The symmetric-key encryption method as claimed in claim 1, wherein the step of generating random number blocks divides a random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said plaintext blocks~~said encryption operation uses one or more said random number blocks whose total length is longer than a length of said ciphertext~~

~~block~~.

3. (currently amended) The symmetric-key encryption method as claimed in claim 2, wherein said plaintext ~~further~~ includes said message, said redundancy data and secret data of a predetermined length, said secret data being generated based on said secret key.

4. (currently amended) The symmetric-key encryption method as claimed in claim 2, wherein said first operation is an exclusive OR operation, said second operation is a multiplication, and said third operation is an exclusive OR operation~~encryption operation performs a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure, combines a plurality of obtained ciphertext blocks, and outputs the combined plurality of ciphertext blocks as ciphertext~~.

5. (original) The symmetric-key encryption method as claimed in claim 2, wherein said encryption operation includes multiplication and addition in a finite field.

6. (original) The symmetric-key encryption method as claimed in claim 2, wherein said encryption operation includes a combination of a cyclic shift operation and arithmetic multiplication.

7. (currently amended) The symmetric-key encryption method as

claimed in claim 2, wherein said symmetric-key encryption method employs a pseudorandom-number generating means for generating said random number sequence based on said secret key; and

wherein said method produces said random number blocks from said random number sequence.

Claims 8-12 (canceled).

13. (currently amended)A symmetric-key encryption apparatus comprising:

a circuit for ~~receiving~~ dividing plaintext composed of a message and redundancy data added to the message~~and a message, and dividing the received plaintext~~ to generate a plurality of plaintext blocks each having a predetermined length~~;~~,

wherein the redundancy data is added to detect whether a ciphertext obtained from said plaintext has been altered;

a random number generation circuit for ~~receiving a secret key to generate a random number sequence, and~~ generating a first random number block and a second random number block both corresponding to each ~~one~~ of said plurality of plaintext blocks based on a secret key that is an input value~~from said random number sequence~~;

an encryption operation circuit for performing encryption operations to produce ciphertext blocks each corresponding to each of said plurality of plaintext blocks; and

a circuit for concatenating the series of said ciphertext blocks one after

another sequentially to output said series as said ciphertext,

wherein said encryption operation circuit for producing the ciphertext block i corresponding to the plaintext i (2 ≤i≤ a number of plaintext blocks) comprises:

a first circuit for performing a first operation on said plaintext block i and said first random number block corresponding to said plaintext block i,

a second circuit for performing a second operation on a result of said first operation performed on said plaintext block i and said first random number block corresponding to said plaintext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said plaintext block i and a result of said first operation performed on said plaintext block i-1, to produce a result of said third operation as said ciphertext block i, and

wherein either said first random number of said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of plaintext blocks or the result of said second operation step.

~~a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and~~

~~an encryption operation circuit for performing an encryption operation using said one of said plurality of plaintext blocks, said random number block, and a feedback value, which was fed back to said encryption operation circuit, obtained as a result of operation on still another one of the plurality of~~

~~plaintext blocks and another random number block, to produce a ciphertext block.~~

14. (currently amended) The symmetric-key encryption apparatus as claimed in claim 13, wherein said random number generation circuit divides a random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said plaintext blocks~~encryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said ciphertext block~~.

15. (currently amended) The symmetric-key encryption apparatus as claimed in claim 14, wherein said plaintext ~~further~~ includes said message, said redundancy data and secret data of a predetermined length, said secret data being generated based on said secret key.

16. (currently amended) The symmetric-key encryption apparatus as claimed in claim 14, wherein said first operation is an exclusive OR operation, said second operation is a multiplication, and said third operation is an exclusive OR operation~~encryption operation circuit includes:~~

~~a circuit for performing a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure; and~~

~~a circuit for combining a plurality of obtained ciphertext blocks, and outputting the combined plurality of ciphertext blocks as ciphertext~~.

17. (original) The symmetric-key encryption apparatus as claimed in claim 14, -wherein said encryption operation circuit performs multiplication and addition in a finite field.

18. (original) The symmetric-key encryption apparatus as claimed in claim 14, wherein said encryption operation circuit includes a cyclic shift operation circuit and an arithmetic multiplication circuit.

19. (currently amended) The symmetric-key encryption apparatus as claimed in claim 14, said random number generation circuit further comprising:

a pseudorandom number generator for generating said random number sequence based on said secret key; and

a circuit for producing said random number blocks from said random number sequence.

Claims 20-24 (canceled).

25. (currently amended) A medium storing a program for causing a computer to perform a symmetric-key encryption method, wherein said program ~~is~~is read into said computer, said program when executed causes said computer to perform~~symmetric-key encryption method comprising~~ the steps of:

~~reading~~ dividing plaintext composed of a message and redundancy data added to the message ~~and a message, and dividing said plaintext~~ to

generate a plurality of plaintext blocks each having a predetermined length,

wherein the redundancy data is added to detect whether a ciphertext obtained from said plaintext has been altered;

~~receiving a secret key to generate a random number sequence, and~~ generating a first random number block and a second random number block corresponding to each ~~one~~ of said plurality of plaintext blocks based on a secret key that is an input value~~from said random number sequence~~;

performing encryption operations for producing ciphertext blocks each corresponding to each of said plurality of plaintext blocks; and

concatenating the series of said ciphertext blocks one after another sequentially to output said series as said ciphertext,

wherein one of said encryption operations for producing the ciphertext block i corresponding to the plaintext block i ($2 \leq i \leq$ a number of plaintext blocks) comprises:

a first operation step for performing an arithmetic computation on said plaintext block i and said first random number block corresponding to said plaintext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said plaintext block i and said second random number block corresponding to said plaintext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said plaintext block i and a result of said first operation step performed on said plaintext block i-1, to produce said ciphertext block i, and

wherein either said first random number of said second random

number is generated in complete isolation from any one of said plurality of plaintext blocks or the result of said second operation step.

~~outputting a feedback value obtained as a result of operation on said one of said plurality of plaintext blocks and said random number block, said feedback value being fed back for use in the operation on another one of the plurality of plaintext blocks; and~~

~~performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks and another random number block to produce a ciphertext block.~~

26. (currently amended) The medium storing a program as claimed in claim 25, wherein the step of generating random number blocks divides a random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said plaintext blocks~~said encryption operation uses one or more said random number block whose total length is longer than a length of said ciphertext block~~.

27. (currently amended) The medium storing a program as claimed in claim 26, wherein said plaintext ~~further~~ includes said message, said redundancy data and secret data of a predetermined length, said secret data being generated based on said secret key.

28. (currently amended) The medium storing a program as claimed

in claim 26, wherein said first operation is an exclusive OR operation, said second operation is a multiplication, and said third operation is an exclusive OR operation~~said encryption operation performs a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure, combines a plurality of obtained ciphertext blocks, and outputs the combined plurality of ciphertext blocks as ciphertext~~.

29. (original) The medium storing a program as claimed in claim 26, wherein said encryption operation includes multiplication and addition in a finite field.

30. (original) The medium storing a program as claimed in claim 26, wherein said encryption operation includes a cyclic shift operation and arithmetic multiplication.

31. (currently amended) The medium storing a program as claimed in claim 26, wherein said symmetric-key encryption method further comprises a step of:

generating pseudorandom numbers to generate said random number sequence based on said secret key; and

wherein said method produces said random number blocks from said random number sequence.

Claims 32-36 (canceled).

37. (currently amended)A program product for causing a computer to perform a symmetric-key encryption method, wherein said program product is read into said computer, said program product comprising:

code for causing said computer to ~~read~~ divide plaintext composed of a message and redundancy data added to the ~~and a~~ message~~, and divide said plaintext~~ to generate a plurality of plaintext blocks each having a predetermined length, wherein the redundancy data is added to detect whether a ciphertext obtained from said plaintext has been altered;

code for causing said computer to ~~receive a secret key to generate a random number sequence, and~~ generate a first random number block and a second random number block both corresponding to each one of said plurality of plaintext blocks based on a secret key that is an input value~~from said random number sequence~~;

code for causing said computer to perform encryption operations for producing ciphertext blocks each corresponding to each of said plurality of plaintext blocks; and

code for causing said computer to concatenate the series of said ciphertext blocks one after another sequentially to output said series as said ciphertext,

wherein one of said encryption operations for producing the ciphertext block i ($2 \leq i \leq$ a number of plaintext blocks) comprises:

a first operation step for performing an arithmetic computation on said plaintext block i and said first random number block corresponding to said plaintext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said plaintext block i and said second random number block corresponding to said plaintext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said plaintext block i and a result of said first operation step performed on said plaintext block i-1, to produce said ciphertext block i, and

wherein either said first random number of said second random number is generated in complete isolation from any one of said plurality of plaintext blocks or the result of said second operation step, and ~~output a feedback value obtained as a result of operation on said one of said plurality of plaintext blocks and said random number block, said feedback value being fed back for use in the operation on another one of said plurality of plaintext blocks; and~~

~~code for causing said computer to perform an encryption operation using said one of the plurality of plaintext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks and another random number block to produce a ciphertext block,~~

wherein said program product is stored in a medium readable by said computer for embodying said codes.